SQUIRE PATTON BOGGS

Ransomware Attacks
Why It Should Matter to Your Business

Ransomware attacks are on the rise. These attacks can be debilitating to business, negatively affecting the organization's productivity, financial performance and brand. Below, we discuss who the malicious actors are targeting, trends in ransomware attacks and the cost of remediation. In follow-up alerts, our team will address methods to increase your IT/cybersecurity posture and the value of cyber insurance, as well as specific issues faced by industries.

For additional information on ransomware, cybersecurity and data protection and privacy, we encourage you to subscribe to our blog, Security & Privacy//Bytes.

The Scene: Experiencing the Unimaginable

Imagine that you walk into your office one morning to find that all employees' computers have been locked, with a threatening message posted on each employee's computer screen demanding a ransom payment in return for the company computer system being unlocked. Your company's data is locked and the backup files have been destroyed. As you scramble to respond to this terrifying scenario, precious time elapses and your business cannot function. Your company is hemorrhaging time, money and customer goodwill, among other things. It is likely that your communication system is down, turning even the simplest coordination into a Herculean task. You are at the mercy of an unseen force – a malicious actor. Your company is a victim of a ransomware attack.

Think this cannot happen to you?

Think again.

Ransomware: Emergence and Proliferation

Ransomware is a type of malicious software, otherwise known as malware, which denies access to a system or data until a set ransom is paid. Ransomware can enter a company's systems through, among other things, contact with an infected website or as a result of a successful phishing email. In many cases, malicious actors infiltrate a company's systems long before they deploy the ransomware. They will then take time to perform reconnaissance on the company's IT infrastructure in order to ensure that their deployed ransomware is targeted to maximize the encryption of data. Once a company's systems are breached, the malicious actor can encrypt them and/or exfiltrate key files, and then will demand a ransom payment, generally in bitcoins, in exchange for the decryption key or restoration of the stolen files. The files in question may contain commercially sensitive information, privileged documents and/or personal information. Ransom demands can range from thousands to millions of dollars in bitcoins.

Everyone Is a Target of Ransomware

A common misperception is that malicious actors, using ransomware, target larger corporations and businesses. In fact, malicious actors, leveraging automated software and other capabilities, target entities of all sizes and in many industries. For example, over the last year, state municipalities, healthcare entities and law firms have all been victims of devastating ransomware attacks. Malicious actors also are targeting non-consumer-facing businesses, such as manufacturing companies. No matter the size or industry, even a slight disruption in operations through the denial of access to key IT systems can result in a company losing thousands to millions of dollars. In fact, earlier this year, Norsk Hydro, a Norwegian aluminum producer, fell victim to a ransomware attack and lost approximately US$52 million as a result. All companies are potential targets. No matter the size of your business or industry sector, your organization is potentially at risk of a ransomware attack.

A Troubling Evolution

Conservative estimates indicate that ransomware has more than doubled over the last year. Some troubling statistics include:

- In 2019, every 14 seconds, an organization will fall victim to ransomware
- 1.5 million new phishing sites are created every month
- Companies are facing an average downtime of 9.6 days after being infected with ransomware
- The average ransomware payment has nearly tripled over the course of 2019, from US$12,762 to US$36,295
- Downtime costs are typically five to 10 times the actual ransom amount, if not greater, as measured by loss in productivity, revenue opportunities, and company reputation

Ransomware statistics show that hackers are focusing more steadily on larger companies that will often pay tens of thousands to millions of dollars to receive their data back. With the increase in ransomware attacks, companies have retained cyber insurance policies to protect themselves. This may be a large reason that malicious attackers are demanding larger ransoms than they did before – they know that vulnerable companies have a greater ability to pay exorbitant ransom demands.

Low-Risk, High-Payoff Criminal Enterprise

Another troubling trend within the ransomware universe is the development of relationships between malicious actors. In many instances, malicious actors skilled in system penetration and infiltration will penetrate a company's systems and then sell that access to other malicious actors, who will then deploy ransomware within that company's systems. These expansive relationships allow malicious actors to grow increasingly sophisticated in their activities (e.g., system penetration, ransomware deployment, etc.). As an example of the growing sophistication of these attacks, once inside a company's systems, many malicious actors are targeting the company's backup systems in order to cripple the company's ability to remediate its systems without paying the ransom. Unable to backup its locked data and systems, the company is at the mercy of the malicious actors and their unreasonable demands. Threats to disclose exfiltrated data are also growing trend and an additional form of digital extortion.

Because malicious actors demand ransom payment through bitcoin, it makes it virtually impossible to trace their location. Hence, malicious actors view ransomware as a low-risk, high-payoff criminal enterprise.

The Cost of Remediation

In addition to the malicious actor's demand for a ransom payment, companies face myriad additional costs associated with responding to a ransomware attack. First, given that responses to ransomware attacks regularly transcend different legal areas and global borders, companies should consider seeking outside counsel in advance in order to be ready to navigate the various legal issues that will need to be dealt with. Briefly, this will assist legal, compliance and security teams to prepare for the following:

- Establishing and maintaining the attorney-client privilege over the response efforts
- Determining whether, when and how to notify law enforcement authorities, data protection authorities, works council, data subjects and/or national security agencies in the case of potential state actors for all impacted countries and jurisdictions
- Analyzing companies' insurance policies and taking appropriate action to maximize coverage
- Responding to authorities' RFIs, internal investigations and enforcement actions
- Minimizing companies' litigation risks and responding to legal actions taken by customers, vendors, partners and authorities

Likewise, companies, through counsel, will likely need to hire an IT firm to remediate its systems, a data forensics firm to contain the malware and conduct an internal investigation to determine the cause of the attack, and a technical intermediary firm to liaise with the malicious actor. Furthermore, companies, through counsel, may have to hire a forensic accounting firm to quantify business interruption costs (which could range from the thousands to millions of dollars) and seek recovery from its insurance carriers (whose policies will need to be carefully reviewed following an attack). Furthermore, companies, through counsel, also may seek to hire public relations firms to remediate any reputational harms with clients, vendors, business partners, and the general public. In sum, while this section is not exhaustive, ransomware attacks can cost substantially more than the ransom payment (should the company make the business decision to pay).

How We Can Help

Our global Data Breach Response team combines experienced cybersecurity, privacy, litigation, government investigations, insurance, and labor and employment specialists working together to provide the technical, legal, regulatory, and procedural advice and support that you need to protect your company and your data.

Our global Data Breach Response team can assist clients by:

- Conducting Cybersecurity Threat Risk Assessments
- Developing and/or reviewing company-specific Cybersecurity Incident Response Plans
- Building Cybersecurity Compliance Programs and Procedures
- Designing and conducting training, including desktop exercises and simulations
- Providing legal support 24/7 to assist clients in responding to ransomware attacks, data breaches, phishing emails, etc.
- Coordinating and drafting breach notifications to data subjects and regulators
- Handling claims from data subjects
- Conducting internal investigations
- Liaising with law enforcement and national security agencies
- Responding to enforcement actions
- Advising on insurance coverage and recovery
- Coordinating with IT professionals and technical consultants on the recovery of data and network remediation
- Supervising forensic investigations and supporting on litigation strategy
- Litigating cybersecurity and data privacy matters
- Working with public relations professionals on crisis management messaging

Our global Data Breach Response team is well equipped to advise and assist your business on all aspects of ransomware response. Our experienced team includes seasoned data protection and litigation experts in the US, the EU and other key markets who will coordinate national and cross-border preparation for, and responses to, cybersecurity and personal data breach threats of all types, including ransomware attacks.

For further information, please contact Colin Jennings.

Contacts

Colin Jennings
Partner, Cleveland
T +1 216 479 8420
E colin.jennings@squirepb.com

Ericka Johnson
Associate, Washington DC
T +1 202 457 6110
E ericka.johnson@squirepb.com

Shalin Sood
Associate, Washington DC
T +1 202 457 6183
E shalin.sood@squirepb.com